IN THE DRAWINGS:

In the Notice of Draftsperson's Patent Drawing Review, the Draftsperson objected to the drawings for failing to comply with 37 C.F.R. 1.84 (g) for containing margins that are unacceptable. Applicants hereby enclose a Transmission of Formal Drawings.

Rejections under 35 U.S.C. § 101:

Claim 40 stands rejected by the Examiner under 35 U.S.C. § 101 as not constituting statutory subject matter. Applicants' respectfully traverse the rejection and submit that Claim 40 constitutes statutory subject matter.

Applicants assert that their invention is an access token and direct the Examiner's attention to the specification, page 16 lines 12 – 19, wherein "an access token includes both device-type tokens ... and logical tokens ...." Applicants' invention is not a token, which is defined as "a unique data object or message that circulates continuously among the nodes of a token ring and describes the current state of the network. Before any node can send a message, it must first wait to control the token." THE MICROSOFT COMPUTER DICTIONARY 444 (4th ed. 1999)

Applicants respectfully request reconsideration and withdrawal of this rejection and allowance of Claim 40.

Rejections under 35 U.S.C. § 112:

Claims 34 and 39 stand rejected by the Examiner under 35 U.S.C. § 112, second paragraph, for failure to further limit the claims. Applicants have amended Claim 34. Applicants have cancelled Claim 39 without prejudice or disclaimer. Applicants request reconsideration and allowance of amended Claim 34.

Rejections under 35 U.S.C. § 103:

Claims 1 – 5, 9 – 42 stand rejected by the Examiner under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,949,882 issued to Michael F. Angelo (hereinafter

"Angelo") and Authoritative Dictionary of IEEE Standards ("IEEE Standards"). Applicants' have cancelled Claim 39 without prejudice or disclaimer. Applicants respectfully traverse and submit Claims 1 – 5, 9 – 38 and 40 – 42, as amended, are patentable over Angelo and IEEE Standards.

Angelo discloses a two piece authentication procedure to enable access to secured computer resources. (col. 3, lines 30-31) The procedure uses a token or smart card "to store an encryption algorithm furnished with an encryption key that is unique or of limited production." (col. 3 lines 37-39) The encryption algorithm is used to encrypt a user-entered password to create a "peripheral" password to permit access to the secured resource. (col. 3, lines 41-48)

Applicants' amended Claim 1 calls for various features including "an executable program code that receives a set of security policies from the access token in the processor in response to the verification data."

Applicants' amended Claim 14 recites a computer system comprising, among other features, an "operating system permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies match an authorization data stored in the nonvolatile memory."

Applicants' amended Claim 26 calls for various steps including "comparing the verification data to the master password and the nonvolatile storage device password for access to the computer system."

Applicants' amended Claim 28 calls for various steps including "authenticating the use of the access token by comparing the password to the security policy."

Applicants' amended Claim 29 call for various steps including "accessing the computer system with a user input password combined with a token access password such that the combined passwords match the one or more security policies configured in the computer system."

Applicants' amended Claim 35 recites a method of using an access token, the method comprising, among other steps, "matching a computer system password with the combined user password and the one or more passwords from the access token."

Applicants' Claim 40 calls for various features including "an access code stored on the access token, wherein the access token transmits the one or more security policies in response to receiving a data stream corresponding to the access code."

Applicants' amended Claim 41 calls for various features including "means for verifying the validity of the access token based on the authentication password."

Applicants' amended Claim 42 recites an information handling system comprising, among other features, "means for verifying the validity of the access token based on the authentication password."

Neither Angelo nor IEEE Standards make obvious Claims 1 – 5, 9 – 38 and 40 – 42, as amended, of Applicant's invention because Angelo or IEEE Standards fails to teach disclose, or suggest all of the elements recited in Claims 1 – 5, 9 – 38 and 40 – 42, as amended. For example, the cited references fail to disclose "an executable program code that receives a set of security policies from the access token in the processor in response to the verification data" as recited in amended Claim 1. As recited in amended Claim 14, Angelo or IEEE Standards fails to disclose, suggest, or teach an "operating system permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies match an authorization data stored in the nonvolatile memory." As recited in amended Claim 26, Angelo or IEEE Standards fails to disclose, suggest, or teach "comparing the verification data to the master password and the nonvolatile storage device password for access to the computer system." As recited in amended Claim 28, Angelo or IEEE Standards fails to disclose, suggest, or teach an "authenticating the use of the access token by comparing the password to the security policy." As recited in amended Claim 29, Angelo or IEEE Standards fails to disclose, suggest, or teach "accessing the computer system with a user input password combined with a token access password such that the combined passwords match the one or more security policies configured in the computer system."

Further, Angelo or IEEE Standards fails to disclose, suggest, or teach "matching a computer system password with the combined user password and the one or more passwords from the access token," as recited in amended Claim 35. As recited in Claim 40, Angelo or IEEE Standards fails to disclose, suggest, or teach "an access code stored on the access token,

wherein the access token transmits the one or more security policies in response to receiving a data stream corresponding to the access code." As recited in amended Claim 41, Angelo or IEEE Standards fails to disclose, suggest, or teach "means for verifying the validity of the access token based on the authentication password." As recited in amended Claim 42, Angelo or IEEE Standards fails to disclose, suggest, or teach "means for verifying the validity of the access token based on the authentication password." Applicants therefore respectfully requests the Examiner to reconsider and withdraw the rejection to and allow Claims 1, 14, 26, 28, 29, 35, and 40 - 42, as amended.

Claims 2 – 5 and 9 – 13 depend from and provide further patentable limitations to amended Claim 1. Claims 15 - 25 depend from and provide further patentable limitations to amended Claim 14. Claim 27 depends from and provides further patentable limitations to amended Claim 26. Claims 30 - 34 depend from and provide further patentable limitations to amended Claim 29. Claims 36 - 38 depend from and provide further patentable limitations to amended Claim 35. Because Claims 1, 14, 26, 28, 29, 35, and 40 - 42, as amended, are deemed allowable, Claims 2 – 5, 9 – 13, 15 – 25, 27, 30 - 34 and 36 - 38 are allowable. Therefore, Applicants respectfully request the Examiner to reexamine, reconsider, withdraw the rejection to and allow Claims 1 – 5, 9 – 38 and 40 – 42, as amended.

Objection to Claims 6 – 8:

Claims 6 – 8 stand objected to by the Examiner as being dependent on a rejected base claim. Applicants have amended Claim 6 – 8 to include the limitations of the base claims. Applicants request withdrawal of the objection and allowance of amended Claims 6 – 8.

III. CONCLUSION

Applicants have now made an earnest effort to place this case in condition for allowance in light of the amendments and remarks set forth above. Applicants respectfully request reconsideration of the rejections and allowance of Claims 1 – 38 and 40 – 42, as amended.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendments. The attached pages are captioned **"Version with Markings to Show Changes Made."** An executed Revocation of Attorney and Appointment of New Attorneys for Non-Provisional Application, with Certificate Under 37 CFR 3.73(b) is also attached hereto.

A Notification of Extension of Time under 37 C.F.R. § 1.136 and § 1.17(a)(1) and a check in the amount of $110.00 to cover the cost for the extension for response within the first month is enclosed. Also enclosed is a check in the amount of $168.00 to cover the cost of two newly added independent claims. Applicants do not believe any additional fee is due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0383 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Thomas R. Felger
Reg. No. 28,842

Date: July 15, 2002

Correspondence Address:
One Shell Plaza
910 Louisiana
Houston, Texas 77002-4992
512.322.2599
512.322.8305 (Fax)

VERSION WITH ~~MARKINGS~~ TO SHOW CHANGES MADE

IN THE SPECIFICATION:

1.0 On Page 9, the paragraph beginning on Line 2 has been amended as follows:

Referring initially to Figure 1, illustrated is a block diagram of a computer system 150 employing an access token 100. The computer system 150 is illustrated as having a central processing unit (or "CPU") 160, **a nonvolatile storage device 195 such as** an ATA-3 type hard disk drive (or "HDD") **[195]**, and an 8051 micro-controller 170. CPU 160 is shown receiving CMOS settings 180 from an area of nonvolatile memory, while the 8051 micro-controller 170 is shown receiving data from nonvolatile memory 190. Access token reader 120 is shown reading access token 100 and providing data to CPU 160 while password or access code 130 is shown entered into input device 140 and transmitted to micro-controller 170. Micro-controller 170 determines if access code 130 is correct and returns a "true" or "false" to CPU 160.

2.0 On Page 9, the paragraph beginning on Line 28 has been amended as follows:

When a person places the access token 100 on the access token reader 120, security software within computer system 150 is invoked and prompts the user to enter the PIN number 130 on an input device **140** **[150]**. The security software program code may be embedded within the basic input-output system that is stored along with the CMOS settings 180 in nonvolatile memory within computer system 150. In this way, the BIOS may operate without exposing data on **nonvolatile storage device** **[HDD]** 195. In one example, the input device 140 is a keyboard upon which the user enters a PIN number. In another example, the input device 140 is a biometric reader that reads biometric data from the user. In a specific example, biometric data is a fingerprint and an input device 140 is a fingerprint reader. Another example of biometric data is eye retina data that is read with an eye scanner. Another example of biometric data is voice data that is spoken into an input device 140, such as a microphone, and compared with a voice print of the user.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

3.0 On Page 31, the paragraph beginning on Line 8 has been amended as follows:

Figure 12 shows an example of a manufacturer preparing access tokens for a customer **1200** **[1100]**. The customer would provide a token request **1201** **[1100]** with policies **1205** **[1105]**, an optional group name **1210**, and a user password request **1215** **[1115]**. Token request **1201** **[1100]** may be for an additional access token for a computer system already received by customer or may be associated with a new computer system request as described in Figure 11 above. Included with the user password request **1215** **[1115]** is the access code 130 shown in Figure 1 containing data the customer desires to use as an access code, or PIN number, associated with the access token. The access code selected by a user could be a PIN number or could include biometric data (i.e., fingerprint data, eye scan data, etc.) the customer wants associated with access token 100. Additionally, the customer may wish to have the manufacturer create a random access code **1225** **[1125]** to include with the access token. After the access code is determined, access token creation **1230** **[1130]** creates the access token by writing the access code to the access token **1235** **[1135]**, and writing policies, group name (if desired), and password data to the access token at step **1240** **[1140]**. Following creation of the access token, the token **1245** **[1145]** is sent to the customer and the access code **1250** **[1150]** (i.e., PIN number) used to verify ownership the access token is sent to the customer. If the token **1245** **[1145]** was created for an existing computer system used by customer, the access code **1250** **[1150]** is mailed separately from the access token so that an unauthorized person does not receive both the token and the code needed to use the token, thus giving the unauthorized person access to the computer system.

IN THE CLAIMS

Please amend Claims 1 –8, 14 – 16, 26, 28, 29, 34 – 36, 41 and 42 as follows:

1. **(Amended)** A computer system comprising:

a processor;

VERSION WITH MARKINGS TO SHOW CHANGES MADE

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that **receives a** set**[s] of** security policies **from the access token** in the processor **in response to the verification data**; and

an executable program code that controls access to resources in the processor based on the security policies.

2. **(Amended)** The computer system of claim 1 further comprising:

a nonvolatile storage device operably coupled to the processor;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the **executable program code receiving valid verification data with the access token provided. [access token reading device reading an access token and the input device receiving verification data.]**

3. **(Amended)** The computer system of claim 2, wherein at least one of the **set of security [one or more]** policies is stored within the nonvolatile storage device password.

4. **(Amended)** The computer system of claim 1, wherein at least one of the **set of security [one or more]** policies is stored on the access token.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

4

5. **(Amended)** The computer system of claim 1 wherein one of the **set of security [one or more]** policies corresponds to the verification data.

6. **(Amended)** **A [The]** computer system **[of claim 1]** **comprising:**

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that sets security policies in the processor, wherein one of the one or more policies includes **a** BIOS control information that is used to configure the computer system**; and**

an executable program code that controls access to resources in the processor based on the security policies.

7. **(Amended)** The computer system of claim 6 wherein the BIOS control information further includes password change information, the password change information including one or more password change settings for a user using the one or more **security** policies.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

8. **(Amended)** A **[The]** computer system **[of claim 1 further]** comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that sets security policies in the processor; and

an executable program code that controls access to resources in the processor based on the security policies; and

a display device, wherein one of the one or more **security** policies includes one or more interface settings that control a desktop presentation on the display device.

14. **(Amended)** A computer system comprising:

one or more processors;

memory electrically interconnected to the one or more processors;

an operating system for controlling the operation of the one or more processors;

an access token communication device electrically interconnected to at least one of the one or more processors**, the access token communication device being communicatively operable with an access token**;

VERSION WITH MARKINGS TO SHOW CHANGES MADE

an input device electrically interconnected to at least one of the one or more processors**, the input device operable to transmit a security code from a user to the one or more processors**;

a nonvolatile storage device electrically interconnected to at least one of the one or more processors, the nonvolatile storage device including a nonvolatile memory;

a set of security [one or more] policies associated with the operating system**[; wherein],** the operating system **[includes] operable to receive the** security code **for** selectively **enabling [enabled by]** the **set of security [one or more]** policies to limit access to the computer system; **and**

the operating system permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies match an authorization data stored in the nonvolatile memory. [responsively to an access token read by the access token communication device.]

15. **(Amended)** The computer system of claim 14 wherein the access token further includes verification data, **the verification data operable to provide the security policies to the nonvolatile memory if the security code matches an authentication code stored in the access token. [wherein the access token is read in response to the input device receiving authentication data corresponding to the verification data.]**

16. **(Amended)** The computer system of claim 14 wherein the operating system includes a BIOS and **[wherein]** the BIOS is stored **in the [on]** nonvolatile memory that is electrically interconnected to the one or more processors.

26. **(Amended)** A method for **accessing [manufacturing]** a computer system, said method comprising:

providing a computer system, the computer system including:

one or more processors;

VERSION WITH MARKINGS TO SHOW CHANGES MADE

a memory operably coupled to the one or more processors;

[one or more images of] an operating system for controlling the operation of the one or more processors;

an access token reading device that is adapted to read **information stored on** an access token;

an input device that is adapted to **[receive]** **transmit** verification data **to the operating system**, the verification data confirming authorized use of the access token;

a nonvolatile storage device operably coupled to the memory;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the access token reading device reading an access token and the input device receiving verification data;

storing a master password on the access token; **[and]**

storing a nonvolatile storage device password on the access token**; and**

comparing the verification data to the master password and the nonvolatile storage device password for access to the computer system.

28. **(Amended)** A method for protecting information stored in an information handling system, said method comprising:

reading an access token **containing a security policy for the information handling system**;

requesting an authentication password from a user;

authenticating the use [verifying the validity] of the access token **by comparing the password to the security policy**;

setting **a** security **policy [policies]** in the information handling system; **and**

unlocking a nonvolatile storage device on the information handling system.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

29. **(Amended)** A method for assembling a computer system, said method comprising:

receiving a list of components for assembling the computer system;

receiving one or more security policies; **[and]**

configuring the computer system using the one or more security policies**; and**

accessing the computer system with a user input password combined with a token access password such that the combined passwords match the one or more security policies configured in the computer system.

34. **(Amended)** The method of claim 29 further comprising:

configuring [preparing] an access token for the computer system**, the access token including the security policies and the passwords associated with the computer system**.

35. **(Amended)** A method of using an access token, said method comprising:

transferring one or more passwords from the access token to a computer system; **and**

receiving a user input password at the computer system and

matching a computer system password with the combined user password and the one or more passwords from the access token.

36. **(Amended)** The method of claim 35 wherein the transferring **step** is **performed** in response to an access code received by the access token.

Please cancel Claim 39 without prejudice or disclaimer.

41. **(Amended)** A computer operable medium for protecting a computer system, said computer operable medium comprising:

means for reading an access token;

means for receiving an authentication password;

VERSION WITH MARKINGS TO SHOW CHANGES MADE

means for verifying the validity of the access token **based on the authentication password**;

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.

42. **(Amended)** An information handling system comprising:

means for reading an access token;

means for receiving an authentication password;

means for verifying the validity of the access token **based on the authentication password**;

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.

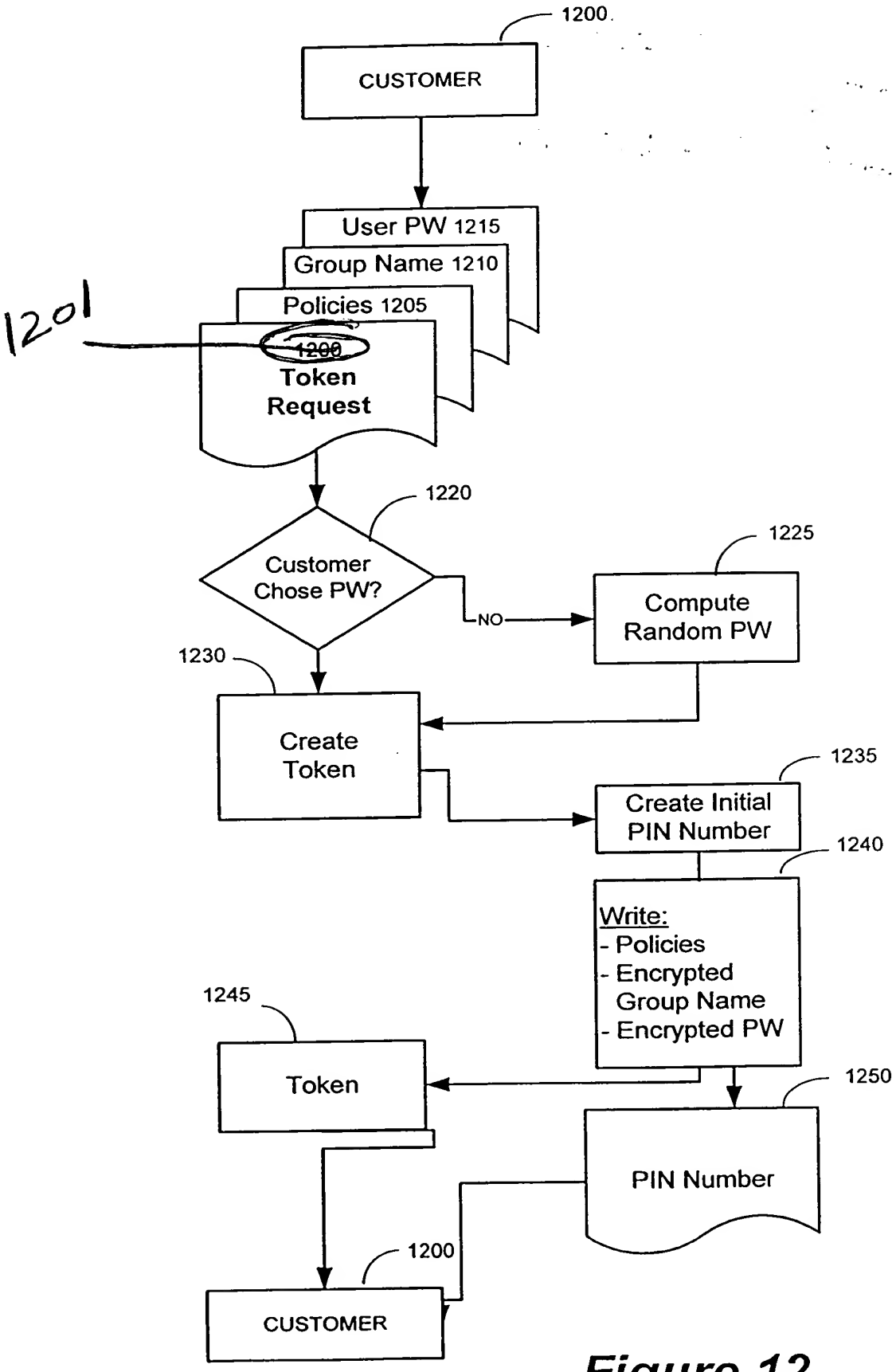
1200
CUSTOMER
User PW 1215
Group Name 1210
Policies 1205
1201
1200
Token Request
1220
Customer Chose PW?
NO
1225
Compute Random PW
1230
Create Token
1235
Create Initial PIN Number
1240
Write:
- Policies
- Encrypted Group Name
- Encrypted PW
1245
Token
1250
PIN Number
1200
CUSTOMER

Figure 12